



## Between The Rock And A Hard Cyber Place

by [Steve Brown](#)

Alcatraz Island sits about 1 mile from San Francisco and it houses an old federal prison. Back in the day, that prison held the likes of gangster Al Capone (Scarface), George Kelly (Machine Gun) and Robert Stroud (The Birdman of Alcatraz). It formally operated as a prison from 1934 to 1963 and is nicknamed "The Rock." It was officially named La Isla de los Alcatraces or Island of the Pelicans in 1775 by a Spanish explorer. We tell you this today so that you have some random information to dump on coworkers or family and friends at this time of year if things get quiet or you are looking to impress.

Alcatraz was designed to keep criminals inside, which is the opposite problem banks are facing today in the cyber world as bankers try to keep criminals out. In fact, the FFIEC recently issued a warning to banks that there has been a rise in both the frequency and the severity of cyber attacks, with many instances now involving extortion. Such attacks can harm your bank in a myriad of ways, from the straightforward loss of liquidity or capital, to reputational harm resulting from fraud or data loss, and even the disruption of service. As a result, community banks need to focus efforts on fending off and mitigating the risks of cyber attacks even more.

Given how quickly malware and ransomware is evolving, protecting sensitive information has become more difficult than ever. An unfortunate reality is that virtually no company, inside or outside of the banking industry, is invulnerable to attack. After all, many attackers are state-sponsored by countries with unlimited resources. Against that onslaught, what can any community bank do? For their part, regulators have tried to provide guidance in this area. They want banks to have programs in place that can effectively "identify, protect, detect, respond to and recover from" cyber attacks. Among the steps banks are encouraged to take are the performance of routine information security risk assessments; ongoing security monitoring, prevention and risk mitigation; implementation of and routine testing of the controls around critical systems; and frequent reviews and updates on incident response and business continuity plans.

Beyond this, regulators also suggest banks focus on the fact that employees can sometimes pose the biggest digital security risk. Because of this, it is equally important to make sure that employees are educated about the potential for cyber attacks and the impact that simple things, such as opening a link within an e-mail from an unverified source can have, or the importance of encrypting sensitive data.

Given how much sensitive information banks exchange and rely on during a typical day, you may also want to consider following the lead of many companies that now forbid employees from using removable USB devices or from accessing any online sites not immediately related to the job function.

Just as employees can inadvertently create breaches, so too can third party vendors. So, when performing security assessments it is also important to factor in the security systems and practices of

your vendors as well. As the Federal Bureau of Prisons learned from Alcatraz, the mere perception that security is not as strong as it needs to be can lead to a whole host of unwanted problems.

## **BANK NEWS**

### **More Vacation**

Research by MassMutual finds 47% of people want more time off from work and 44% want better company matching of their 401(k).

### **Marketing**

According to iAcquire, 70% of mobile searches lead to action on a website within 1 hour of searching.

### **No Taxes**

CNBC reports The Tax Policy Center finds the number of US households that don't pay federal income taxes is 45.3% or about 77.5mm.

### **Health Insurance**

The Wall Street Journal reports the Obama administration now says many consumers will see noticeable premium increases when buying health coverage on insurance exchanges in 2016. Officials say so-called silver plans will see 7.5% increases on average and 60% of enrollees will see the average rate for a base plan rise by 6.3%.

### **Consolidation**

The Wall Street Journal reports about 33% of all industries in the US are operating in an environment considered to be highly concentrated under antitrust laws vs. only 25% in 1996.

### **Job Gone**

Job site CareerCast projects that jobs most likely to become obsolete due to technology and other factors in the next 7Ys are: tailoring (-4%); insurance underwriters (-6%); drill press operator (-6%); flight attendant (-7%); logging (-9%); jeweler (-10%); newspaper reporter (-13%); farmer (-19%); meter reader (-19%); and mail carrier (-28%).

### **Tough Savings**

A survey by BlackRock finds 74% of Americans surveyed said they find it difficult to keep on top of bills while saving for retirement.

### **Drones**

Wal-Mart has joined Amazon in asking the FAA for permission to test drones for home package delivery. Wal-Mart says 70% of the US population is within 5 miles of one of its stores.

### **Robo Advisors**

Cerulli predicts the market for digital investment advice will climb to \$489B in assets under management in the next 5Ys vs. \$18.7B today.

### **Social Phones**

Facebook reports an average of 844mm mobile active daily users.

### **High Failure**

The Startup Genome report finds 90% of internet start-ups fail within 3Ys.

### **Retirement Borrowing**

Research by Fidelity Investments finds 24% of people who took loans out against their 401(k) saved less in the 1st year the loan was taken out, while 15% stopped saving entirely within 5Ys of taking out the loan.

*Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.*